

Jun 07, 2023

s/ Erin Hayes

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of)

(Briefly describe the property to be searched)
(or identify the person by name and address))information associated with certain accounts that are stored at premises)
owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an)
electronic communications service and/or remote computing service)
provider headquartered at One Apple Park Way, Cupertino, California.)

Case No. 23-m-381 (SCD)

Court Case No. 23-CR-68

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

Please see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Please see Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 6-21-23 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Stephen C. Dries
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of

Date and time issued: 6-7-23 2:25 pm

Stephen C. Dries

Judge's signature

City and state: Milwaukee, WI

Honorable Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 60%;"> <div style="text-align: center; margin-bottom: 10px;"> <p>_____</p> <p><i>Executing officer's signature</i></p> </div> <div style="text-align: center;"> <p>_____</p> <p><i>Printed name and title</i></p> </div> </div> </div>		

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with accounts, realswiper2900@icloud.com, rio.dinerojr@icloud.com and kinglow722@icloud.com, that are stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. (“Apple”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers

(“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, **from June 1, 2022 to May 31, 2023**, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, **from June 1, 2022 to May 31, 2023**, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and

query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **fourteen days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities, of violations of Title 18 U.S.C. § 1951(a), Hobbs Act Robbery, Title 18 U.S.C. § 924(c), Brandishing of a Firearm during a Crime of Violence, and Title 18 U.S.C. §1708, Mail Theft those violations involving that HUSSEIN A. HAJI (XX/XX/2001)), HURIA H. ABU (XX/XX/2002), JESSIE L. COOK (XX/XX/2003), ABDI A. ABDI, (XX/XX/2001), DARRION ALLISON and others and occurring after **June 1, 2022**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Mail theft, conspiracy to commit mail theft or fraud, illegal entry to mailboxes, stolen USPS arrow keys, wire fraud, identity theft, bank fraud, armed robbery, or any other illegal activities relating to the information described in this affidavit.
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with the user ID about matters relating to the violations listed above including records that help reveal their co-actors, locations of illegal activities, communications related to illegal activities and evidence of the illegal activities included in this affidavit.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Jun 07, 2023

s/ Erin Hayes

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*

information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California.

Case No. 23-m-381 (SCD)

Court Case No. 23-CR-68

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Please see Attachment A.

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. §1951(a)	Hobbs Act Robbery
18 U.S.C. §924(c)	Brandishing a Firearm during a Crime of Violence
18 U.S.C. §1708	Mail Theft

The application is based on these facts:

Please see attached Affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Applicant's signature


Heather Wright, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

TELEPHONE *(specify reliable electronic means)*.

Date: 6-7-23


 Judge's signature

City and state: Milwaukee, WI

Honorable Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Heather Wright being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by Apple Inc. (“Apple”), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since July of 2010. Since August of 2020, I have been assigned to the FBI’s Milwaukee Area Violent Crimes Task Force, a multi-jurisdictional law enforcement entity charged with investigating violations of federal law, including bank robberies, commercial robberies, armed motor vehicle robberies, and other violent crime matters, defined under Title 18 of the United States Code. I have been trained in a variety of investigative and legal matters, including the topics of Fourth Amendment searches, the drafting of search warrant affidavits, and probable cause. I have participated in criminal investigations, surveillance, search warrants, interviews, and debriefs

of arrested subjects. As a result of this training and investigative experience, I have learned how and why violent actors typically conduct various aspects of their criminal activities.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that HUSSEIN A. HAJI (XX/XX/2001), HURIA H. ABU (XX/XX/2002), JESSIE L. COOK (XX/XX/2003), ABDI A. ABDI, (XX/XX/2001), DARRION ALLISON and others, committed the armed robberies of United States Post Office mail carriers on October 25, 2022, near 2650 N. Martin Luther King Drive, Milwaukee, on December 7, 2022, near 3205 N. Bremen Street, Milwaukee, on February 10, 2023, near 5273 N. 27th Street, Milwaukee, and on March 13, 2023, near 4548 N. 38th Street, Milwaukee. These offenses are in violation of Title 18 U.S.C. § 1951(a), Hobbs Act Robbery, Title 18 U.S.C. § 924(c), Brandishing of a Firearm during a Crime of Violence, and Title 18 U.S.C. §1708, Mail Theft. There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. On October 25, 2022, the Milwaukee Police Department responded to an armed robbery complaint at 2650 N. Martin Luther King Drive, Milwaukee, Wisconsin. Upon arrival,

officers spoke with the victim, identified as a United States Postal mail carrier, hereinafter referred to as D.D. D.D. stated that he had been conducting his route at approximately 2:30 P.M., and was about to start at 2500 N. Richards Street, when he was approached by four young males. D.D. described Subject #1 as possibly a Hispanic male, approximately 19 years old. D.D. stated that Subject #1 and three other males, approached him from behind and demanded that he “give up his shit.” D.D. stated that he heard one of the subjects say that they had a gun to his back. D.D. stated that he told the subjects that he was not going to give them anything and quickly turned around to face the attackers, fearing that one of them may have a gun. D.D. stated that he did not observe any of the subjects with a firearm and immediately took a fighting stance. Three of the subjects ran away, while Subject #1 stayed and took a fighting stance as well. D.D. stated that as Subject #1 attempted to punch D.D., D.D. attempted to punch Subject #1. D.D. stated that he was unsure if his punch made contact with Subject #1, however, Subject #1 staggered back and ran away. D.D. stated that Subject #1 ran eastbound and eventually northbound towards the alley. D.D. stated that he chased after Subject #1, however, he lost sight of Subject #1 and returned to his vehicle. D.D. stated that when he returned to his vehicle, he was unable to find his USPS issued Arrow key that had been hanging around his neck on a lanyard.

7. On January 28, 2023, a photo array was presented to D.D. with the target of the photo array as JESSIE L. COOK (dob: 12/22/2003). D.D. identified COOK as the individual that had demanded his things and attacked D.D. on October 25, 2022.

8. On December 7, 2022, the Milwaukee Police Department responded to 3205 N. Bremen Street, Milwaukee, Wisconsin, for an armed robbery of a United States postal mail carrier, hereinafter referred to as E.V. E.V. stated that at approximately 3:00 p.m., he had just finished delivering mail to 3219 N. Bremen Avenue and was walking south towards the next block when

he passed two subjects who were walking northbound on the west sidewalk. E.V. stated that after they had passed, he could hear running footsteps approaching him from behind and he turned around. The same two subjects that had just passed him ran up to him and one had a gun pointed at him.

9. E.V. stated that Suspect #1 said “Gimme everything..gimme everything...gimme everything,” while pointing a small framed semi-automatic hand gun at him. E.V. stated that he provided his ID and keys that were on a lanyard around his neck as well as the mail in his hands. E.V. stated that the key fob for the postal van as well as his Arrow key were on the key ring that was provided. The Arrow key was specifically assigned to E.V. that day and can open the blue mail boxes and some boxes at apartment buildings. E.V. stated that the serial number for the key provided was #30411. E.V. stated that Subject #2 took the ID with the keys attached but dropped the mail E.V. had handed to him. E.V. stated that he attempted to hand the Subjects his mail bag because it had scanned devices within the bag that could be GPS located, however, the subjects were not interested and were only interested in the lanyard and keys. E.V stated that he then ran to a corner bar for safety and called the police. E.V stated that the subjects ran southbound and heard a car squeal off in a hurry.

10. Shortly after the incident, a witness approached him and told him that he saw the suspects get into a white Nissan Murano. That particular witness could not stay on scene. However, an additional witness also came forward and stated that they had observed the robbery and corroborated that she, too, had observed the suspects enter a white Nissan Murano.

11. A canvas for video surveillance was completed and video surveillance from a Ring doorbell was obtained at 3219 N. Bremen Street. After a review of the video, Subject #1 was observed to be a black, male, late teens, approximately 5’10” tall, thin build, dark complexion,

wearing a black hoody, black mask (above eyes showing), light gray pants, black shoes, armed with a black semi-automatic handgun. Suspect #2 was observed to be a black, male, late teens, approximately 6'0" tall, thin build, medium complexion, wearing a black hoody, black mask (above eyes showing), black pants, white shoes, unknown if armed.

12. On January 27, 2023, a state residential search warrant related to a drug investigation was executed at 2519 N. Buffum Street, Milwaukee, Wisconsin. Prior to the execution, two black males, and two black females were observed leaving the residence in a blue Toyota Camry. Shortly thereafter and just prior to the warrant execution, the blue Toyota returned with two of the four individuals inside. When officers approached the vehicle, they identified the individuals as MARVIN TURNER (dob: XX/XX/2000) and HUSSEIN A. HAJI (dob: XX/XX/2001). Officers then executed the search warrant and identified HURIA H. ABU (dob: XX/XX/2002), JESSIE L. COOK (dob: XX/XX/2001), AMAURIE D. SMITH (dob: XX/XX/2005) as well as two females who were not residents of the house, hereinafter "S. J". and "S. W.". A search of the residence resulted in the recovery of a Glock 19 handgun (stolen out of Cudahy), a loaded Ruger P95 handgun, a loaded Ruger PC Charger carbine pistol, a loaded AK 7.62 cal pistol, a GSG rifle upper with mock silencer, hundreds of pieces (approximately 900 checks) of stolen mail including personal and commercial checks from Milwaukee, Shorewood, Brookfield, Brown Deer, as well as others, checks currently being "washed" in acetone, keys on a bed, located in a bedroom, that unlocked a safe which contained \$7000, (1) USPS arrow key, (1) set of USPS keys, (20) cellular telephones, and (2) laptop computers. Officers also located keys for a Nissan Murano that unlocked a white Nissan Murano parked outside the residence and matched the vehicle description used in the October 25, 2022 and December 7, 2022 robberies.

13. Following the arrests of HAJI, COOK, ABU, SMITH and TURNER, interviews were conducted. During the interview of COOK, COOK stated to detectives that he was the primary user of the Nissan Murano located at the residence during the execution of the search warrant. COOK admitted to being involved in the robbery of the postal carrier on October 25, 2022. COOK stated that COOK was the individual that punched the postal carrier during the robbery, however, COOK would not state why the mail carrier was targeted or who he was with during the robbery. COOK stated to detectives, that he was the owner of a Samsung Galaxy 20 black cellular phone with telephone number 262-389-0018.

14. During the interview of HAJI, HAJI stated to detectives that he was the owner of a purple Apple iPhone 14 and a yellow Apple iPhone XR with the telephone number 262-364-4059. HAJI stated that his service provider was T-Mobile and that he has had that cellular number for a couple of months. During the interview, HAJI admitted to detectives that he had participated in the robbery of the mail carrier that had occurred on December 7, 2022. HAJI stated that ABU was the driver, and that COOK had the gun and pointed it at the white mail carrier. HAJI stated that they used the Nissan Murano, and that HAJI was the individual that took the arrow key from the mail carrier. HAJI also admitted to Detectives that they were after the specific arrow key that mail carriers carry during the robbery. HAJI stated that HAJI, COOK, and ABU participated in “mail runs”, which are when a person removes mail from mailboxes. HAJI stated that he has participated in approximately 40 mail runs in at least four different vehicles. HAJI stated that the target of the mail runs are personal checks and that they sell them after they are located. HAJI stated that one of the methods of payment when selling the checks is CashApp. HAJI stated that the day he was arrested, he was taken into custody outside of the residence because he had been inside the Toyota. HAJI stated that his firearm was located inside the Toyota on the passenger side floorboard. HAJI

stated that he has owned the firearm for approximately one year and purchased it at the Shooter's club. HAJI stated that the last time he shot the gun was on New year's outside the house at 2519 N. Buffum Street at midnight on New Year's Eve. HAJI stated that he had fired the gun into the air.

15. During the interview of S. J., S.J. stated that she had only been to the house on Buffum twice and that she had seen guns in the house. S.J. stated that she had seen approximately four guns. S.J. stated that she heard SMITH and others talking about a robbery and that S.J. believed they were talking about the robbery of a mailman. S.J. raised her hands up simulating holding a gun and stated that he said "nigga up" or something like that.

16. During the interview of S.W. stated that ABU, COOK and HAJI do "mail runs" in the morning. S.W. sated that she believed that they get checks out of the mail using the arrow key obtained by the postman. S.W. did not know who robbed the mail person to get the key but she believed that ABU, COOK, and HAJI were the ones that did the robbery because they were the ones who do the mail runs. S.W. stated that ABU, COOK, and HAJI take pictures of the checks but she was unsure if it was before or after they put the checks in acetone. S.W. stated that SMITH had been involved with ABU, COOK and HAJI lately and had been riding in vehicles and doing the "check stuff" with them. S.W. stated that SMITH had been staying on the couch at the house.

17. On February 2, 2023, a Wisconsin state search warrant was obtained for all the cellular phones seized during the search warrant executed at 2519 N. Buffum Street. A review of the phones indicated that FBI evidence item 1B1 and evidence item 1B2 were phones associated to HAJI. Evidence item 1B1 was described as an iPhone A2651 14 Pro Max, purple in color with no case with PIN code "000000". Evidence item 1B2 was described as an iPhone XR A1984, gold in color, with PIN code "2900". A review of evidence item 1B1 and 1B2, were consistent with

photos and instant messages associated to HAJI. Numerous messages located within HAJI's phone indicated that HAJI had obtained an arrow key, was using the arrow key to open mailboxes, steal personal checks from unwilling victims, and re-writing the checks to bank accounts associated to HAJI or another that HAJI had recruited to deposit the stolen check. There were also messages within HAJI's phone, dating back to June of 2022, where HAJI is soliciting individuals via social media to obtain co-actors with bank accounts where HAJI can deposit stolen checks. Also, during the review of the phones, it was determined that HAJI used the iCloud account realswipper2900@icloud.com.

18. On February 10, 2023, the Milwaukee Police Department responded to an armed robbery that had occurred near 5273 N. 27th Street, Milwaukee, at approximately 11:40 A.M. The victim was identified as a United States Postal carrier, hereinafter referred to as N.M. N.M. stated that N.M. had been working mail route 88, had parked his mail vehicle near 2626 W. Rhor, and walked to the door to deliver the mail. N.M. stated that as he began to approach the residence of 5273 N. 27th Street from the north, he walked onto the small porch to place mail into the boxes. N.M. stated that he then observed three subjects come from the backyard (from the west of where he was) and surrounded him as he was on the porch. N.M. stated that he was somewhat trapped due to the railings on the porch and the three subjects surrounding him. N.M. stated that he had the ring of apartment keys in one pocket of his outer most jacket and the chain was exposed across his jacket leading to the Arrow key that was in the opposite pocket of his jacket.

19. N.M. described Subject #1 as a black male, approximately 22-27 years old, over 6'0" tall, medium brown complexion, wearing a black ski mask covering his head, face and neck, with his eyes exposed, aviator sunglasses with plastic frames and gray/black lenses, a black hooded sweatshirt, dark jeans, unknown shoes, armed with a black Glock 9mm handgun with an extended

magazine. N.M described Subject #2 as a black, male, approximately 22-27 years old, over 6'0" tall, medium brown complexion, wearing a black ski mask covering his head, face and neck with his eyes exposed, "beach style" square sunglasses, a black hooded sweatshirt, dark blue jeans, unknown shoes, armed with a black Glock 9mm handgun with a tan extended magazine and switch attached to the back of the gun. N.M. stated that N.M. knew the term "switch" to be an added part on a gun that makes the firearm fully automatic. N.M. described Suspect #3 as a black, male, approximately 22-27 years old, over 6'0" tall, medium brown complexion, wearing a black ski mask covering his head, face and neck, with his eyes exposed, a black hooded sweatshirt, dark jeans, unknown shoes, armed with a black Glock 9mm handgun with an extended magazine.

20. N.M. stated that Suspect #1 was armed with a gun which he held at his side when he demanded N.M.'s keys. N.M. stated that he held up his hands while Suspect #1 grabbed the chain that was exposed outside of his jacket and took N.M.'s keys. N.M. stated that Suspect #2 approached him, used his gun to push up the brim of N.M.'s hat, and asked N.M. what else he had. N.M. stated that he told the suspect that he didn't have anything else. N.M. stated that Suspect #3 did not say anything to him or touch him, but was armed with a gun in his waistband and positioned himself with the other two Suspects. N.M. stated that after the suspects obtained N.M.'s keys, all three suspects fled on foot in the same direction they had approached. N.M. stated that he heard car doors opening and a vehicle drive away but he did not look into the alley to obtain a vehicle description nor which direction they fled.

21. A canvas for surveillance video was conducted and Ring video was located at 5248 N. 27th Street as well as surveillance video from 2800 W. Custer Ave. During the collection of the Ring video, officers were able to observe at 11:41AM, a white 2007-2012, 4 door, Nissan Altima driving southbound through the alley at a high rate of speed. The vehicle had tinted windows

(including front window brow only), a sunroof, side window deflectors, six spoke aluminum rims (split spokes), damage to rear passenger bumper/quarter panel, damage to front passenger quarter panel, dual exhaust, and front and rear unknown registration plates. During a review of the surveillance video obtained from 2800 W. Custer, Officers observed the white Nissan Altima approach the alley at 11:38 A.M., from the west and drive southbound in the alley. Multiple suspects can be observed exiting the vehicle and proceed towards where the victim was robbed. The white Nissan continues southbound in the alley following the incident.

22. On February 13, 2023, at approximately 2:52 P.M., a law enforcement member of the Milwaukee Area Violent Crimes Task Force (MAVCTF) observed a vehicle matching the above description driving west on North Avenue from 73rd Street. The vehicle was a 2010 Nissan Altima 4 door (WI plate AJF-7039). The vehicle subsequently pulled into the Brother's Plus Grocery Store located at 4020 W. North Avenue. Task Force Officers (TFOs) observed a thin black male with shoulder length dreads exit the vehicle's front passenger door and enter the business. The subject was wearing a black T-shirt, camouflage pants, and white/black shoes. The subject then exited the store and re-entered the Altima's front passenger door. TFO Strasser obtained a short video of the subject during the course of the surveillance.

23. The vehicle was then observed driving to and parking in the rear 2225 N. 35th Street. Task Force Officers were able to run the plate and noted that the vehicle listed to ABDI BABA (dob: 01/01/1998), with an address of 2303 W. Cherry Street. This same vehicle was observed via a law enforcement camera system at West Silver Spring Drive and North Green Bay Avenue on February 10, 2023, at 11:08 A.M. The robbery occurred on February 10, 2023, at approximately 11:41 A.M and is 0.9 miles away from the West Silver Spring Drive and North Green Bay Avenue intersection.

24. Task Force Officers were aware of the several armed robberies of United States Postal carriers of their Arrow keys in recent months and that a search warrant had been executed on January 27, 2023. Task Force Officers were also aware that following the search warrant, ABU had been interviewed by MAVCTF TFO Brendan Dolan. TFO Dolan was shown the short video clip of the surveillance of the subject that was observed getting in and out of the Nissan Altima. TFO Dolan was able to identify the subject as ABU based on his prior interactions with him.

25. On February 14, 2023, a state search warrant was obtained for a GPS tracker in order to identify location information for the 2010 Nissan Altima 4 door (WI plate AJF-7039) which was identified by law enforcement as the suspect vehicle in the February 10, 2023, armed robbery. On Friday March 3, 2023, a GPS was attached to the vehicle and the GPS began providing location information. Along with officers observing and locating the vehicle at 2303 W. Cherry Street in order to place the GPS onto the vehicle, during the monitoring of the GPS, Task Force Officers observed the vehicle and monitored the vehicle's GPS location at the Cherry Street address on numerous occasions.

26. On March 13, 2023, law enforcement members of the MAVCTF and Milwaukee Police Officers responded to an armed robbery of a United States Postal carrier near 4548 N. 38th Street, Milwaukee. The victim, identified and hereinafter referenced as M.P., stated that at approximately 1:00 p.m., he parked his truck at 4501 N. 38th Street on the west side of the street, facing south. M.P. stated that while delivering mail at 4514 N. 38th Street, he observed two black male suspects on the west side of the street walking southbound. M.P. stated that the two seemed suspicious because they had masks on. M.P. stated that the two suspects walked past his truck, then walked in front of his truck eastbound. The suspects then went north on the east side of N.

38th Street. M.P. stated that he later observed them duck by the houses near 4518 N. 38th Street while he was further north delivering mail.

27. M.P. stated that when he got near 4548 N. 38th Street, he observed the two suspects running at him. M.P. described Suspect #1 as a black, male, approximately 16 years old, approximately 5'4" tall, short, thin build, wearing a dark royal blue coat, black running pants, armed with a Draco styled gun with a wooden stock. M.P. described Suspect #2 as a black, male, approximately 6'0" tall, light complected, wearing a black jacket and black jogging pants. M.P. stated that one of them stated "don't run now bitch." M.P. stated that Suspect #1 pointed the gun at his head and said, "Give me the keys. Give me the keys. I'll shoot you." M.P. stated that they tried grabbing his keys from the right side of him, but they were on a lanyard. M.P. stated that he told them that the keys were on a lanyard, so they unclipped them and ran northbound from the location and continued eastbound on W. Glendale.

28. A witness to the incident, hereinafter P.M., stated that she heard talking outside and looked out her front window and observed the postal carrier running. She stated that she got up to the storm door and observed two suspects, one of which had a gun pointed at the postal carrier and was wearing a blue coat. P.M. stated that she heard the postal carrier say "ok..ok" but did not hear what the suspects were saying. P.M. stated that she then grabbed her three-year-old nephew and pulled him to the ground for fear that shots would be fired. P.M. stated that she waited for the suspects to leave and called the police.

29. Video surveillance was obtained from the Hopkins Food Mart located at 4601 N. Hopkins Street, Milwaukee. The cameras were located on the south side of the business and the east side of the business. MAVCTF investigators observed a 2009 silver Honda Civic with front and rear plates, no sunroof, damage to front driver's quarter panel, 7 spoke hubcaps, broken front

driver hubcap, with the front passenger inner headlight on (others defective), circling the block and fleeing the area of the robbery, just after it took place.

30. An attempt to identify the vehicle was conducted by querying FLOCK and ALPR cameras in the area with a similar suspect vehicle description. A hit on a 2009 Honda Civic 4 door, WI plate ABG-8200, was obtained at several times on March 13, 2023 at the following locations:

- a. 16:26 – 21 SWE W. Fond Du Lac at Capital Ave.
- b. 13:36 – #01 N/B Port Washington @ Hampton Ave
- c. 12:19 – #10 MLK & W North – S/B
- d. 11:42 – 25 S/B N. Sherman at W Hampton
- e. 8:33 – 07 S/B N. 35th Street at W. Wisconsin

31. The vehicle listed to a Mohammed F. Omar (dob: XX/XX/1990) of 1809 W. McKinley Avenue, Milwaukee.

32. A Milwaukee Police database query was then done for the Wisconsin plate ABG-8200. A call for service regarding a subject with a gun and shots fired was received on January 2, 2023 near North Buffum Street and East Wright Street. A second caller then called and reported that her house had been struck by gunfire at 2513 N. Buffum Street. Officers responded and ran all vehicles in the area including a silver 2009 Honda Civic, WI plate ABG-8200, which was parked in front of 2519 N. Buffum Street (next door to 2513 N. Buffum, and also struck by the gunfire) when officers arrived. A body camera review of the responding officer was reviewed by investigators and the 2009 silver Honda was also observed driving by the officer at 10:42 a.m. on January 2, 2023.

33. On March 14, 2023, an offline search of the 2009 Honda Civic, WI plate ABG-8200 was done, and on December 19, 2022, the vehicle was run by Whitefish Bay Police

Department. Your affiant contacted Whitefish Bay Police Department on March 14, 2023 and confirmed with Whitefish Bay Detective Joe McLeod that the vehicle was traffic stopped on December 19, 2022 at 9:48 p.m., at the intersection of Santa Monica and W. Silver Spring Drive in Whitefish Bay, for speeding, driving without a license, and failure to stop at a stop sign. The driver of the vehicle was identified as HURIA H. ABU, dob: XX/XX/2002. ABU provided Whitefish Bay with a home address of 2519 N. Buffum Street. During a review of the body cam of Whitefish Bay officers during the traffic stop, ABU can be observed speaking with officers in the driver's seat of the vehicle. During the interaction, ABU was observed holding a cellular telephone with a red case. ABU provided officers with the cellular telephone in order to provide a photo of his identification card. Again, the cellular telephone can be seen being handed to the Whitefish Bay officer by ABU in a red case. The cellular telephone is then handed back to ABU by the officer. ABU also provided officers with his home address of 2519 N. Buffum Street in Milwaukee.

34. Following the arrest of COOK, ABU, SMITH, TURNER, and HAJI, on January 25, 2023, only COOK and HAJI were held in state custody. All others were released and on February 10, 2023, the next robbery of a United States Postal carrier for his Arrow key occurred. The suspect vehicle in that robbery was the 2010 Nissan Altima 4 door (WI plate AJF-7039) registered to BABA who is associated to ABU. ABU was observed on February 13, 2023, exiting the Altima during a law enforcement surveillance. The suspect vehicle of the United States Postal carrier robbery on March 13, 2023 was identified as a 2009 Honda Civic 4 door (WI plate ABG-8200). ABU was stopped by Whitefish Bay Police Department on December 19, 2022, driving this suspect vehicle.

35. On March 24, 2023, surveillance was conducted by the FBI Surveillance Operations Group of the 2009 silver Honda Civic. FBI SOG members observed the driver of the vehicle, later identified as ABDI A. ABDI, dob: XX/XX/2001, exit the Honda Civic at the Fast and Friendly Grocery Store located at 311 W. Locust Street, Milwaukee. FBI SOG members observed ABDI exit the location and return to his vehicle. While walking to his vehicle, FBI SOG members took photographs of ABDI exiting the location and were able to observe what appeared to be registration plates and a registration sticker in his left hand.

36. Later that same day, a traffic stop of the silver 2009 Honda Civic was conducted by the Milwaukee Police Department for expired registration tags affixed to the vehicle. The driver of the vehicle was identified as ABDI. ABDI indicated to officers that the vehicle was registered in his name and he had just obtained new plates and registration for the vehicle. ABDI indicated that the new plates for the vehicle were WI plate ASV-4406. Officers observed two other occupants inside the vehicle and identified the individuals as ABU and DARRION M. ALLISON, dob: XX/XX/2000. While officers were obtaining contact information for the individuals inside the vehicle, ABU indicated that his telephone number was 262-264-0206, ABDI indicated that his telephone number was 262-283-2100, and ALLISON indicated that his telephone number was 414-588-5392. Officers then released the vehicle without incident.

37. On March 27, 2023 at 12:20 am, Butler Police Department (BPD) Officer Knapp observed a suspicious vehicle, later identified as a silver 2009 Honda Civic, parked on the west side of N. 125th Street facing south (near the Butler Post Office), with a defective head lamp and dark tinted windows. Officer Knapp ran the registration of the vehicle, WI plate ASV-4406, and the registered owner came back to ABDI, with a listed address of 5230 N. Sherman Blvd #23 in

Milwaukee. A DOT check of ABDI revealed that ABDI had a suspended license for a failure to pay a forfeiture.

38. Officer Knapp turned his marked squad around and the vehicle pulled away from its parked position southbound N. 125th Street towards W. Hampton Avenue. As he was attempting to catch up to the vehicle to conduct a traffic stop for an equipment violation, Officer Knapp observed a male subject, later identified as ABDI, running from the west side of N. 125th Street across N. 125th Street, eastbound in the alley behind Butler Auto Care, 12432 W. Hampton Avenue and south of 4820 N. 125th Street. While checking the area, Officer Knapp located ABDI and the other male subject, identified verbally as DARRION M. ALLISON, dob: XX/XX/2000, walking northbound on the west side of the street through the snow along N. 124th Street in front of 4935 N. 124th Street.

39. After losing sight of both subjects, Officer Knapp regained eyes on the subjects and made contact with the individuals, who verbally identified themselves as ABDI and ALLISON. ALLISON told Officer Knapp that they were trying to get to the store. Officer Knapp then spoke to ABDI and asked why someone else was driving his vehicle. ABDI told Officer Knapp that everyone was “good” and indicated that his cousin was driving his vehicle with his permission. Upon obtaining ABDI and ALLISON’s identifying information, ABDI stated that his telephone number was 262-283-2100 and ALLISON indicated that his telephone number was 414-588-5392. Officer Knapp then indicated to ALLISON and ABDI that they were free to leave.

40. After ABDI and ALLISON were released, Officer Knapp, again checked the area and observed the suspicious 2009 Honda Civic return. Officer Knapp activated his emergency lights and conducted a traffic stop on N. 125th Street, just south of W. Stark Street. Officer Knapp made contact with the driver, identified as HURIA H. ABU, dob: XX/XX/2002, and informed him

of the reason for the traffic stop. Officer Knapp smelled a strong odor of marijuana inside the vehicle. ABU stated that he was in the area to obtain gas and that he was just “chilling” there and that “I always park right here.” Prior to walking back to his squad vehicle, ABU told Officer Knapp that Officer Knapp could check the vehicle out. Officer Knapp then searched the vehicle via consent from ABU. Officer Knapp located a box of blue latex gloves, 21.9 grams of a green leafy substance that later field tested positive for THC, a black and multicolor backpack containing a black Nike ski mask and (17) personal checks made out to various individuals issued from various individuals, most of whom resided in the City of Milwaukee. Officer Knapp also located (55) unused “cannabis flower” Ziplock bags, a box of 9mm Federal ammunition containing (20) unused round, a black and red digital scale, and (2) additional checks in the glovebox, along with (2) money orders totaling \$150 USC.

41. Officer Knapp also located (4) Apple iPhones inside the vehicle. One of the Apple iPhones had a red/black case with ALLISON’s driver’s license in the case pocket on the back side of the phone. The second iPhone (blue back with no scratches or cracks) was in the same spot that ALLISON’s iPhone was located. This phone appeared to be brand new and not set up. The third phone was an iPhone that had a silver back with no case. This was the cellular phone on ABU’s person when he exited the vehicle and placed it on the trunk of the vehicle. When the home screen turned on, there was a picture of ABU wearing a white T-shirt with black pants holding money. The fourth iPhone located, had a blue cracked back and pieces missing along with the lower front screen that was cracked. This phone was on the front passenger seat. There were no identifying serial numbers or model numbers observed on the outside of this phone. This phone was not in a case.

42. Following the search of the vehicle. ABU was taken into custody and cited for possession of marijuana as well as possession of drug paraphernalia. ABU was transported to the Waukesha County Jail for booking and then released.

43. Later that day, on March 27, 2023, Officer Knapp went back to the area of the location where ABDI and ALLISON had been questioned and observed (2) blue latex gloves on the east side of 4935 N. 124th Street. One of the blue latex gloves was located on the south side of the driveway entrance and the second glove was located on the north side of the driveway entrance.

44. On March 28, 2023, after speaking with your affiant about the circumstances regarding the investigation on ABU as well as others, BPD Captain Brian Zalewski obtained video surveillance from the Village of Butler Town Hall. Captain Zalewski reviewed Village of Butler Town Hall security cameras during the timeframe of Officer Knapp's contact with ABU, ALLISON and ABDI. At 12:18:30 AM, the camera activated (as it is motion censored) as two subjects were observed next to, on the north side of, the blue mailbox in front of the Post Office. One subject was squatting down and appeared to be tampering with the bottom half of the mailbox. The second subject, who was the taller of the two, was standing behind the first subject. It should be noted that the blue mailbox had the lock and key access on the lower half of the side of the box facing north. At 12:18:32 AM, the subject squatting down stands up and both subjects began to walk towards N. 125th Street. The camera stopped recording at 12:18:45 AM.

45. Following a review of video surveillance, Captain Zalewski contacted the post master of the Butler Post Office, Karen Monreal, located at 12420 W. Hampton, one block from where the 2009 Honda Civic was parked the previous morning when ABU was arrested. Captain Zalewski stated that Monreal stated that the top of the bin in the front mailbox contained numerous small packages, election ballots, and a small amount of mail located underneath the packages,

however, based on her many years of experience working at this post office, the bin in the mailbox would normally be overflowing after the weekend. On that day, she considered the amount of mail lighter than the normal load.

46. On March 28, 2023, prior to returning the aforementioned cellular phones that were recovered from the Honda Civic to their owners, Captain Zalewski called the telephone numbers provided by ALLISON and ABDI and the associated cellular telephone did ring and confirm that the cellular number provided by ALLISON and ABDI, were indeed, the telephone numbers assigned to those cellular telephones. Captain Zalewski then called the telephone number provided by ABU as his cellular telephone number, however, the cellular phone in the custody of BPD, and seized from ABU, did not ring.

47. On April 23, 2023 and into April 24, 2023, Members of the Milwaukee Area Violent Crimes Task Force were involved in the surveillance of known mailboxes that have experienced mail thefts. Postal Inspector Chris MASSARI provided information that the mailboxes at 5995 N Teutonia Ave (City and County of Milwaukee) and 5521 W Center St (City and County of Milwaukee) had both been targeted and had mail stolen from them.

48. On April 23, 2023, at approximately 11:15PM, officers observed two males running eastbound on W Florist Ave towards N Teutonia Ave where there were known USPS mailboxes. Suspect 1 was tall, possibly 6'00" to 6'03" with a medium build, wearing dark pants, a dark hooded sweatshirt with the hood up, and possible writing on the front of the sweat shirt. Suspect 1 was later identified as ALLISON. Suspect 2, was short, possibly 5'05" to 5'07" wearing what appeared to be an Adidas jacket or sweatshirt. The jacket or sweatshirt was dark or black with stripes going down the shoulders ending at approximately the elbow area. Suspect 2 was later identified as

ABDI.

49. ALLISON acted as a lookout as ABDI crouched down and opened the mailbox located at 5995 N Teutonia Ave. The mailboxes can only be opened with an Arrow Key. The suspects removed what appeared to be mail from the mailbox and then fled westbound on W Florist Ave where they got into a dark colored Chevrolet Malibu, with no rear plate, parked on the south side of W Florist St in the 3400 block and then fled westbound..

50. At approximately 12:00AM, FBI Analyst Emily SLAJUS observed via a live stream video feed, the same two subjects go to the mailboxes at the post office located at 5521 W Center St, in Milwaukee, open the mailboxes, appear to take the mail, and then flee. FBI Analyst Slajus then communicated this to undercover MAVCTF surveillance units. Task Force Officer Michael SKEMP (Brookfield PD) and FBI Special Agent Ian BYRNE were in an undercover vehicle and were travelling north on Sherman Blvd from W Wright St and responded to the area. TFO SKEMP called out the vehicle over Milwaukee Police Radio and a traffic stop was conducted.

51. The driver of the vehicle was identified as ALLISON and the front passenger was identified as ABDI. ABDI and ALLISON were arrested and taken into custody without incident. Following a search of ALLISON's person for officer safety, an Arrow Key with serial number 77-32733 on it was located in ALLISON's front left pocket which matched the key stolen during the March 13th armed robbery. A search of the vehicle was conducted by members of the MAVCTF. The Chevrolet Malibu's listed owner was ABU and was registered to the address of 2519 N Buffum Street. Inside of the glovebox of the Malibu were two pieces of mail addressed to ABU. In the front passenger seat, where ABDI had been seated, were two large black plastic garbage bags containing approximately 400-500 pieces of mail. Also located within the vehicle, were

multiple bank cards, two personal checks, a box of blue latex gloves, and a box of black garbage bags in the trunk of the vehicle.

52. On Monday, April 24, 2023, members of the MAVCTF observed ABU exit the Clark gas Station located at 2242 N. 12th Street in Milwaukee and enter a light blue Chrysler 200 with no plates. ABU was observed entering the driver's seat of the vehicle and drove east on North Avenue. A traffic stop of the Chrysler was conducted and ABU was taken into custody without incident.

53. In a Mirandized interview, ALLISON admitted to being a part of the robbery on March 13, 2023 at 4548 N 38th St in the City and County of Milwaukee. He said that robbery occurred because a few nights prior ABDI was using a different Arrow Key to get mail from mailboxes and the key broke off in the mailbox. ALLISON stated that ABU was extremely upset about this and threatened ABDI to get another key. ALLISON explained that ABU was known as "The Don" and was the leader of this group that steals mail, alters and cashes checks and robbed mail carriers for their USPS Arrow Keys. ALLISON stated that they refer to ABU as "the Don" but ABU preferred to be called "Wiz.". Following ALLISON's arrest, ALLISON's phone was recovered in the console of the vehicle and during the search of the vehicle, ALLISON was receiving a number of missed telephone calls from an individual saved in ALLISON's phone as "Wiz". ALLISON stated he believed that ABU would have hurt or killed ABDI if he did not get a new key.

54. ALLISON further stated that on March 13, 2023 he had met up with ABDI, ABU, LAZARUS JONES and DESHAWN ROBINSON. ALLISON stated that he was driving the Honda and ABDI was in the back seat while ABU followed them in a Malibu. ALLISON stated

that they drove around and eventually found a mail carrier. ALLISON stated that ABU then got into the Honda and JONES got into the Malibu. ALLISON stated that they then circled back around and he (ALLISON), ABDI, and ROBINSON went and robbed the mail carrier at gunpoint. ALLISON stated that ABDI had a Draco styled pistol that had been provided by ABU. ALLISON said ABDI found the key in the mail carriers' bag and pulled them out. After taking the keys, ALLISON stated that ABDI "racked" the Draco AK-47 and was scared that ABDI was going to shoot the mail carrier. ALLISON stated that they ran back to the vehicle after doing the robbery. ALLISON stated that as soon as they entered the vehicle, ABDI handed over the Arrow Key and the Draco styled pistol back to ABU. ALLISON stated that ABDI and ABU were all laughing about the robbery then. ALLISON said they did the robbery under the direction of ABU. ALLISON provided consent for law enforcement to search his phone that was located inside the Chevrolet Malibu at the time of his arrest. ALLISON described his cellular phone as a red iPhone in a black case.

55. In a Mirandized interview, ABU admitted to being present for the March 13th armed robbery and admitted knowing there would be a robbery for an Arrow Key. ABU also admitted to being the driver and look out during the December 7, 2022 armed robbery. ABU further admitted being present for the February 10, 2022 armed robbery and acknowledged that an Arrow Key was taken. ABU stated several times during the interview that he did not commit the robberies but that he was "party to a crime." ABU provided a consent to search for the cellular phone that was seized from his person at the time of his arrest.

56. Following his arrest, ABU's jail calls were monitored by members of the MAVCTF. During one of the monitored jail calls, that was placed by ABU on April 26, 2023,

ABU told a female, believed to be his girlfriend, to “hop on” his iCloud account and lock his phone. ABU told the female that his iCloud account was rio.dinero@icloud.com and provided the female with his password. The female tried to login but it didn’t work. ABU stated that he couldn’t remember what his iCloud account was but was sure about the password. ABU told the female that he was very concerned about the contents of his iCloud account and to take down all of his accounts because law enforcement had his phone. ABU then told his girlfriend to text “Maurie” (believed by law enforcement to be AMAURIE SMITH) and tell “Maurie” to login to ABU’s iCloud account from “Maurie’s” phone because ABU had previously logged into his iCloud account from “Maurie’s” phone. Law enforcement was able to confirm that “Maurie” was AMAURIE SMITH based on future calls made to SMITH by way of three way calling through ABU’s girlfriend.

57. On May 9, 2023, I reviewed the contents of the cellular phone associated to ABU. I reviewed numerous messages as well as the accounts associated to the primary user of the cellular phone and observed that the user account associated to the cellular phone that ABU stated was his, and provided consent for, was rio.dinerojr@icloud.com.

58. On May 25, 2023, I reviewed the contents of cellular phone associated to ALLISON. I reviewed messages as well as the accounts associated to the cellular phone that ALLISON stated was his and provided consent. The iCloud associated to ALLISON was determined to be kinglow722@icloud.com.

59. Based on these facts, I believe that the iCloud account realswiper2900@icloud.com was created and used by HAJI and that it contains evidence, instrumentalities, contraband, identities of co-actors, and fruits of these crimes essential to this investigation. I also believe that the iCloud account rio.dinerojr@icloud.com was created and used

by ABU and that it contains evidence, instrumentalities, contraband, identities of co-actors, and fruits of these crimes essential to this investigation. I also believe that the iCloud account kinglow722@icloud.com was created and used by ALLISON and that it contains evidence, instrumentalities, contraband, identities of co-actors, and fruits of these crimes essential to this investigation

BACKGROUND CONCERNING APPLE¹

60. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

61. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”)

¹ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

62. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

63. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated

with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

64. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

65. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access

services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

66. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

67. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

68. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

69. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

70. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the violations of Title 18 U.S.C. § 1951(a), Hobbs Act Robbery, Title 18 U.S.C. § 924(c), Brandishing of a Firearm during a Crime of Violence, and Title 18 U.S.C. § 1708, Mail Theft. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

71. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

72. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

73. Based on the forgoing, I request that the Court issue the proposed search warrant.

74. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with accounts, realswiper2900@icloud.com, rio.dinerojr@icloud.com and kinglow722@icloud.com, that are stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. (“Apple”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers

(“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, **from June 1, 2022 to May 31, 2023**, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, **from June 1, 2022 to May 31, 2023**, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and

query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **fourteen days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities, of violations of Title 18 U.S.C. § 1951(a), Hobbs Act Robbery, Title 18 U.S.C. § 924(c), Brandishing of a Firearm during a Crime of Violence, and Title 18 U.S.C. §1708, Mail Theft those violations involving that HUSSEIN A. HAJI (XX/XX/2001)), HURIA H. ABU (XX/XX/2002), JESSIE L. COOK (XX/XX/2003), ABDI A. ABDI, (XX/XX/2001), DARRION ALLISON and others and occurring after **June 1, 2022**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Mail theft, conspiracy to commit mail theft or fraud, illegal entry to mailboxes, stolen USPS arrow keys, wire fraud, identity theft, bank fraud, armed robbery, or any other illegal activities relating to the information described in this affidavit.
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with the user ID about matters relating to the violations listed above including records that help reveal their co-actors, locations of illegal activities, communications related to illegal activities and evidence of the illegal activities included in this affidavit.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple Inc. (“Apple”), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple’s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature